REMARKS

Claim 1, 8, 11, 18, 19, 25, 27, 28, 30 and 32 are amended. Claims 1-33 are pending for consideration. In view of the foregoing amendments and the following remarks, Applicant respectfully requests that this application be allowed and forwarded on to issuance.

§112 Rejections

Claims 18, 19, and 27 stand rejected under 35 U.S.C. §112 as failing to provide an antecedent basis for an element in the claims. All three claims have been amended to provide proper antecedent basis, thus obviating the Office's ground for this rejection.

§101 Rejections

Claims 1-12, 25, 27-30, and 32-33 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Although Applicant traverses the rejection, Applicant has amended the claims for the sole purpose of advancing prosecution. Applicant respectfully submits that such amendments obviate the §101 rejections.

First, the Office rejects claims 1-12 as being directed to a "form of energy". (*Office Action of 05/19/06*, p. 3). Without assenting to the propriety of the rejection and without waiver of the original claim language, Applicant has amended base claim 1 to recite "A processor-readable medium <u>having a tangible component</u>". Applicant thus submits that amended claim 1 defines statutory subject matter in accordance with 35 U.S.C. §101.

Next, the Office rejects claims 25, 27-30, and 32-33 as allegedly being directed to non-statutory subject matter. The Office states that these claims recite computers and servers comprising software modules "per se". Thus, according to the Office, these claims are directed neither to "computer components nor statutory processes". (*Office Action of 05/19/06*, p. 3). Applicant respectfully disagrees. Nevertheless, Applicant has amended base claims 25, 28, 30, and 32 to recite computers or servers "having a tangible component". Applicant thus submits that these claims recite statutory subject matter—namely machines— under 35 U.S.C. §101. For further support, Applicant cites to the Office's Final Computer Related Examination Patent Guidelines, which state that "[i]f a claim defines a useful *machine* or manufacture by identifying the physical structure of the machine or manufacture in terms of its *hardware or hardware and software combination*, it defines a *statutory product*." §IV.B.2.a. (emphasis added). Thus, Applicant respectfully submits that claims 25, 27-30, and 32-33—directed to computers or servers with modules—define statutory subject matter.

Finally, the Office further rejects claim 30 under 35 U.S.C. §101 for failing to "achieve a tangible result." According to the Office, claim 30 "merely recites a database and a distribution module for distributing software, [while] no physical transformation occurs as [a] result of distributing." *Id.* Again, Applicant respectfully disagrees. Instead, claim 30 recites a "distribution server having a tangible component" and comprising a "distribution module". The Guidelines thus dictate that this claim is directed to a "statutory product", as it "defines a useful *machine* or manufacture by identifying the physical structure of the machine or manufacture in terms of its *hardware or hardware and software combination*. §IV.B.2.a. (emphasis added). Applicant therefore requests that the rejection be withdrawn.

§102 Rejections

Claims 1-18 and 20-33 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,199,204 to Donohue. Applicant respectfully traverses the rejections as discussed below.

Claim 1 recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (emphasis added):

- receiving a binary signature;

- receiving a security patch;

- ***identifying a vulnerable binary file*** on a computer based on the binary signature; and

- ***updating the vulnerable binary file*** on the computer with the security patch.

Donohue, meanwhile, describes an updater agent that is associated with a computer program and that accesses relevant network locations to download and install updates to the agent's associated program. The agent downloads and installs the updates if those updates satisfy predefined update criteria of the updater agent. (*Donohue*, abstract). The predefined criteria may include the time period between searches for updates and whether the computer user has selected to receive all updates or only certain ones. In a preferred embodiment, the updater agent searches the internet via a search engine to find the network location where an update list is kept. Donohue's updater agent then *compares available software updates with installed software on the computer to determine which updates are relevant*. The updater agent then compares these updates with the predefined

criteria to determine whether or not to download the updates. *Id.* at column 4, line 14 through column 5, line 10.

Applicant respectfully submits that Donohue does not disclose "identifying a vulnerable binary file". In stating that Donohue does indeed show such an element, the Office cites to column 8, lines 45-60. The Office then claims that Donohue's "retrieved file 160" discloses Applicant's "vulnerable binary file", and that the cited passage discloses "identifying a vulnerable binary file on a computer based on the binary signature". For convenience, Applicant reproduces this passage below:

> The updater component uses the URL to access 220 the list 60 and downloads 230 a file 160 comprising the portion of the list 60 of available updates which relates to the particular product. The updater component then performs steps 240-280 as shown in FIG. 4. Each file 160 contains message digests (e.g. MD5) which are digitally signed. The retrieved file 160 is then analyzed 240 using a digital signature checking algorithm (such as the algorithm described in U.S. Pat. No. 5,231,668). This is important to verify that the file 160 represents the correct software updates list for the particular software product, and that the file has not been tampered with since signing. Also, checking for the digital signature is a useful way of filtering the results of the search since these may include a plurality of Web page URLs other than the correct one (the search may find other pages which have a reference to the named product version, including pages not published by the software vendor). If an attempt to download and verify a file is not successful, then the updater component moves on to the next URL found in the search.

Applicant respectfully submits that this passage does not teach the element for which the passage is cited. Here, the updater agent navigates to a software vendor's website to find a list of relevant updates. The "file 160" that the Office refers to is the portion of the list of updates that relates to the updater agent's

software. This portion of the updates list is not, however, a "*vulnerable* binary file on a computer". (emphasis added). It is instead a list of updates. Applicant respectfully submits that this list has not been shown to be "vulnerable" in any way.

In fact, Applicant respectfully submits that the Donohue system is quite inapposite of the subject matter of Applicant's claim. In Donohue, the agent searches for a "file 160" of updates, the updates to be performed on the agent's associated program. These updates are *not* to be performed on the file 160 of updates for which the agent searched. Applicant's claim, meanwhile, recites "*identifying a vulnerable binary file* on a computer based on the binary signature; and *updating the vulnerable binary file* on the computer with the security patch." (emphasis added). In sum, Donohue's system identifies updates that are available for a particular computer program while Applicant's claim identifies the "vulnerable…file" itself.

For at least this reason, this claim is allowable.

Furthermore, Applicant respectfully submits that the rejection is improper for failing to show how Donohue discloses the "updating" element of Applicant's claim.

Applicant submits that if the above logic of the Office is followed, then *Donohue's file 160 must be "updat[ed]" in order to disclose Applicant's claim.* In other words, If Donohue's "file 160" is the "vulnerable binary file" as Office suggests, and which Applicant does not concede, then in order to disclose Applicant's claim the updater agent would also have to update the file 160. This is true because Applicant's claim recites "updating *the* vulnerable binary file". Applicant submits, however, that the updater agent does not update the update list,

but rather updates the agent's associated program. Applicant also notes that the updater agent, located on a computer, would obviously not have the authority to update an update list located on a software vendor's website. Applicant finally notes that while the Office cites to a different portion of Donohue for this "updating" element, such additional citation does not solve the above infirmity, as Applicant's claim recites "updating *the* vulnerable binary file" and the Office cites Donohue's file 160 as *the* "vulnerable binary file".

Thus, for at least this additional reason, this claim is allowable.

Claims 2-7 depend from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 8 recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (emphasis added):

- *receiving a binary signature that identifies a security vulnerability in a binary file*;

- receiving a security patch configured to *fix the security vulnerability in the binary file*; and

- distributing the binary signature and the security patch to a plurality of servers.

In making out a rejection of this claim, the Office states that Donohue discloses all of the elements of Applicant's claim. In stating that Donohue

discloses "receiving a binary signature that identifies a security vulnerability in a binary file" the Office chiefly relies on column 8, lines 45-50.

As discussed above in regards to claim 1, however, Applicant respectfully submits that this portion of Donohue does not serve to anticipate this element of Applicant's claim. Applicant once again submits that Donohue's file 160, comprising a list of updates, *does not disclose a binary file with "a security vulnerability"*. In fact, the Office fails to show how Donohue's list of updates is at all vulnerable. Applicant respectfully submits that because this file 160 is not vulnerable at all, and thus the cited passage of Donohue cannot be shown to disclose "receiving a binary signature that identifies *a security vulnerability in a binary file*", as recited in Applicant's claim.

For at least this reason, Applicant respectfully submits that this claim is allowable.

Furthermore, Applicant respectfully submits that the cited portion of Donohue also fails to disclose "receiving a security patch configured to fix the security vulnerability in the binary file". As discussed at length in regards to claim 1, if Donohue's file 160 is cited to disclose *the* "binary file" of Applicant's claim, then the security patch must be "configured to fix the security vulnerability" in Donohue's file 160 (i.e. *the* binary file). Applicant submits, however, that Donohue has not been shown to fix any security vulnerability in the updates list, nor would the updater agent have the authority to do so.

For at least this additional reason, Applicant respectfully submits that this claim is allowable.

Claims 9-10 depend from claim 8 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited

features which, in combination with those recited in claim 8, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 11, as amended, recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (emphasis added):

- receiving a binary signature from a server;

- *searching for the binary signature in binary files located on a client computer*;

- sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature;

- receiving the security patch from the server; and

- *updating the binary file on the client computer* with the security patch.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. Namely, Donohue does not disclose "searching for the binary signature in binary files located on a client computer". Instead, Donohue has *at most* been shown to disclose an updater agent located on a computer and that retrieves a list of updates from various software vendor websites. Furthermore, Donohue does not disclose "updating the binary file on the client computer", as the Donohue updater agent does not disclose updating the update list, as discussed above.

For at least these reasons, Applicant respectfully submits that this claim is allowable.

Claim 12 depends from claim 1 and is allowable as depending from an allowable base claim. This claim is also allowable for its own recited features which, in combination with those recited in claim 11, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 13 recites a method comprising (emphasis added):

- receiving a binary signature;

- *searching for a vulnerable file* based on the binary signature;

- if a vulnerable file is found, requesting a security patch; and *fixing the vulnerable file with the security patch*.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. Namely, Donohue does not disclose "searching for a vulnerable file". Instead, Donohue at most has been shown to search for a list of updates. Furthermore, Donohue has also not been shown to disclose "fixing the vulnerable file", as the list of updates has not been shown to be "fix[ed]...with the security patch."

For at least these reasons, Applicant respectfully submits that this claim is allowable.

Claims 14-18 depend from claim 13 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited

features which, in combination with those recited in claim 13, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 20 recites method comprising (emphasis added):

- receiving a binary signature and a security patch from a distribution server;

- ***searching on a client computer for a vulnerable file*** associated with the binary signature; and

- if a vulnerable file is found, ***fixing the vulnerable file with the security patch***.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. Namely, Donohue does not disclose "searching on a client computer for a vulnerable file". Donohue has also not been shown to disclose "fixing the vulnerable file with the security patch."

For at least these reasons, Applicant respectfully submits that this claim is allowable.

Claims 21-22 depend from claim 20 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 20, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 23 recites a computer comprising (emphasis added):

- means for receiving a binary signature;

- ***means for searching for a vulnerable file*** based on the binary signature;

- means for requesting a security patch if a vulnerable file is found; and

- ***means for fixing the vulnerable file with the security patch***.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. Namely, Donohue does not disclose "means for searching for a vulnerable file". Donohue has also not been shown to disclose "means for fixing the vulnerable file with the security patch".

For at least these reasons, Applicant respectfully submits that this claim is allowable.

Claim 24 recites a server comprising (emphasis added):

- means for receiving a binary signature and a security patch from a distribution server;

- ***means for scanning a client computer for a vulnerable file*** associated with the binary signature; and

- ***means for fixing the vulnerable file with the security patch*** if a vulnerable file is found.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. Namely, Donohue does not disclose "means for scanning a client computer for a vulnerable file". Donohue has also not been shown to disclose "means for fixing the vulnerable file with the security patch."

For at least these reasons, Applicant respectfully submits that this claim is allowable.

Claim 25 recites a computer having a tangible component and comprising (emphasis added):

- binary information;

- *a scan module configured to receive a binary signature and scan the binary information* for the binary signature; and

- a patch module configured to request a security patch and install the security patch if the binary signature is found in the binary information.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. Namely, Donohue does not disclose "a scan module configured to receive a binary signature and scan the binary information". Applicant notes that both the "binary information" and the "scan module" are recited to be a part of the computer. Applicant further notes that Donohue has not been shown to disclose a scan

module on a computer that is configured to scan information that is also part of the computer. At most, Donohue has been shown to describe an updater agent that searches software vendors' websites.

For at least these reasons, Applicant respectfully submits that this claim is allowable.

Claims 26-27 depend from claim 25 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 25, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 28 recites a computer having a tangible component and comprising (emphasis added):

- binary files;

- a binary signature; and

- *a security patch module configured to receive the binary signature from a server and to scan the binary files in search of the binary signature.*

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. Namely, Donohue does not disclose "a security patch module configured to receive the binary signature from a server and to scan the binary files in search of the binary signature". Applicant notes that both the "binary files" and the "security patch

module" are recited to be a part of the computer. Applicant further notes that Donohue has not been shown to disclose a security patch module on a computer that is configured to scan files that are also part of the computer. At most, Donohue has been shown to describe an updater agent that searches software vendors' websites.

For at least these reasons, Applicant respectfully submits that this claim is allowable.

Claim 29 depends from claim 28 and is allowable as depending from an allowable base claim. This claim is also allowable for its own recited features which, in combination with those recited in claim 28, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 30 recites a distribution server having a tangible component and comprising (emphasis added):

- *a database; and*

- *a distribution module* configured to receive a binary signature and a security patch, store the binary signature and the security patch in the database, and distribute the binary signature and the security patch to a plurality of servers.

In making out a rejection of this claim, the Office states that Donohue anticipates all of the elements of the claim and cites to various portions of the reference. First, the Office cites to repository 40, shown in Donohue's Figure 1, as disclosing Applicant's "database". The Office then cites to portions of Donohue discussed above in regards to claim 1 and other independent claims. These passages include column 8, lines 45-60, column 7, lines 60-62, column 5, lines 5-7, and

column 7, lines 55-65. (*Office Action of 5/19/06*, p. 11). Applicant respectfully

traverses the rejection.

Applicant respectfully submits that Donohue has not been shown to disclose

Applicant's claim 30. More specifically, the Office fails to show a distribution

server comprising *both* "a database; *and* a distribution module", as recited in

Applicant's claim. (emphasis added). Instead, the Office cites to a user's

conventional network-connected computer system 10 as containing Applicant's

claimed "database", in the form of repository 40. The Office then appears to cite to

remote server systems 50' as containing Applicant's claimed "distribution module".

The computer system 10 and remote server system 50', however, *do not comprise a*

single "distribution server" as recited in Applicant's claim. In fact, they could not

be much further apart, emphasized by Donohue's characterization of server system

50' as "remote". Donohue's Figure 1 depicts this deficiency, and is reproduced

below:
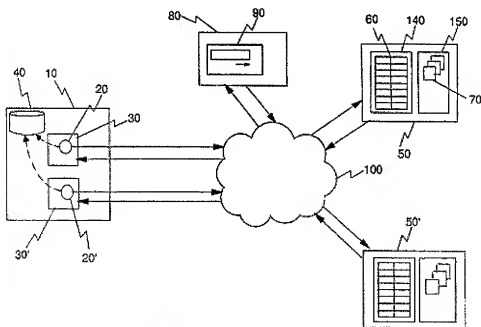
FIG. 1

As shown above, Donohue does not disclose a "distribution server" comprising *both* a "database; *and* a distribution module", as recited in Applicant's claim. Instead, this portion of Donohue shows two wholly distinct components connected by a network 100, such as the Internet.

For at least this reason, Applicant respectfully submits that this claim is allowable. This claim is also allowable for at least all of the reasons discussed above in regards to claim 1.

Claim 31 depends from claim 30 and is allowable as depending from an allowable base claim. This claim is also allowable for its own recited features which, in combination with those recited in claim 30, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Claim 32 recites a server having a tangible component and comprising:

- a binary signature associated with a security vulnerability in a binary file;

- a security patch configured to fix the security vulnerability in the binary file; and

- *a scan module configured to scan binary files on a client computer for the binary signature and to update the binary file* with the security patch if the binary signature is found.

In making out a rejection of this claim, the Office states that Donohue anticipates and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that Donohue does not anticipate this claim. Namely, Donohue does not disclose "a scan module configured to scan binary files on a

client computer for the binary signature and to update the binary file". Again, Donohue has not been shown to scan any files on a "client computer". Instead, the reference has at most been shown to search for software vendors' websites.

For at least these reasons, Applicant respectfully submits that this claim is allowable.

Claim 33 depends from claim 32 and is allowable as depending from an allowable base claim. This claim is also allowable for its own recited features which, in combination with those recited in claim 32, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

§103 Rejections

Claim 19 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Donohue in view of U.S. Patent No. 5,930,504 to Gabel. Applicant also respectfully traverses this rejection.
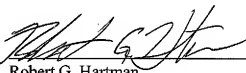
Claim 19 ultimately depends from independent claim 13. As discussed above, Applicant submits that claim 13 is allowable. Furthermore, in the rejection of claim 19 Gabel has not been cited to remedy the deficiencies of the rejection of base claim 13. Thus, claim 19 is allowable as depending from an allowable base claim. This claim is also allowable for its own recited features which, in combination with those recited in claim 13, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

Conclusion

All of the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully submitted,

Dated: 08/21/06

By: _____

Robert G. Hartman
Reg. No. 58,970
(509) 324-9256 ext 265